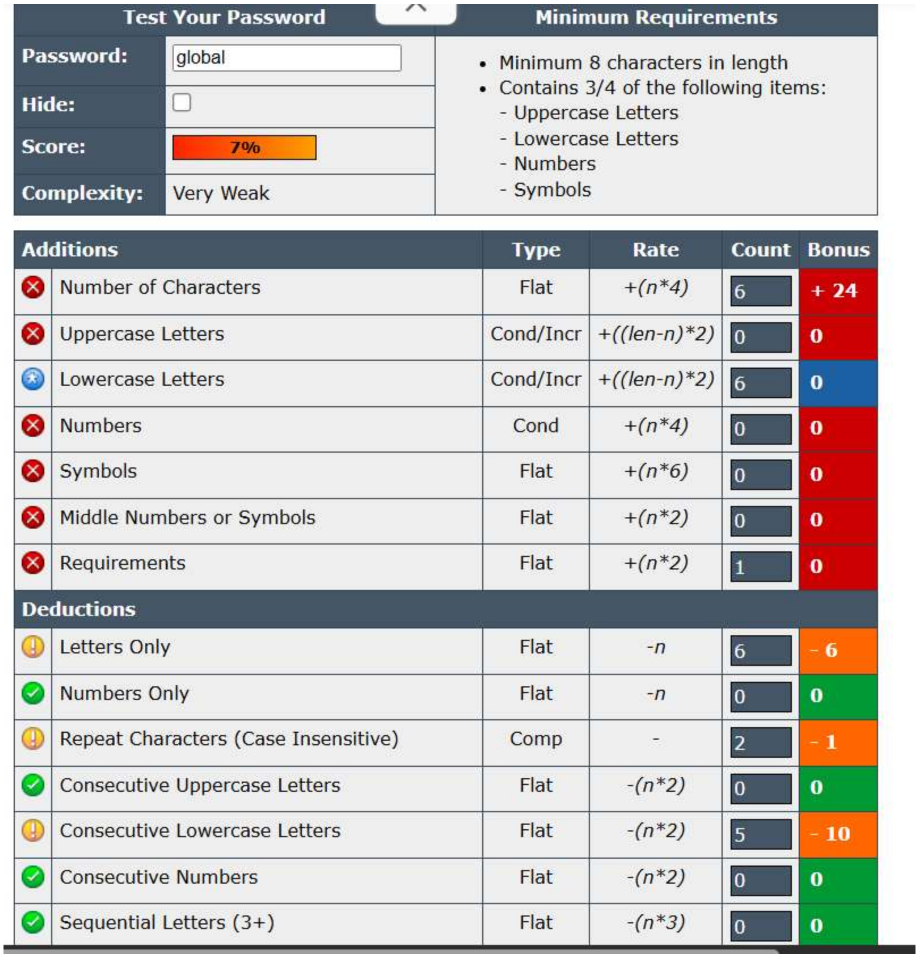
Password Strength Evaluation Report

his report details the findings from an evaluation of password strength using an online password strength checker, as outlined in the internship task. The objective was to understand what makes a password strong and how different components, such as length and character types, affect its security. Three passwords were tested to demonstrate the difference between a weak, a good, and a strong password.

Password 1: "global"

- **Score**: 7%
- **Complexity**: Very Weak



Test Your Password	
Password:	global
Hide:	☐
Score:	7%
Complexity:	Very Weak

Minimum Requirements

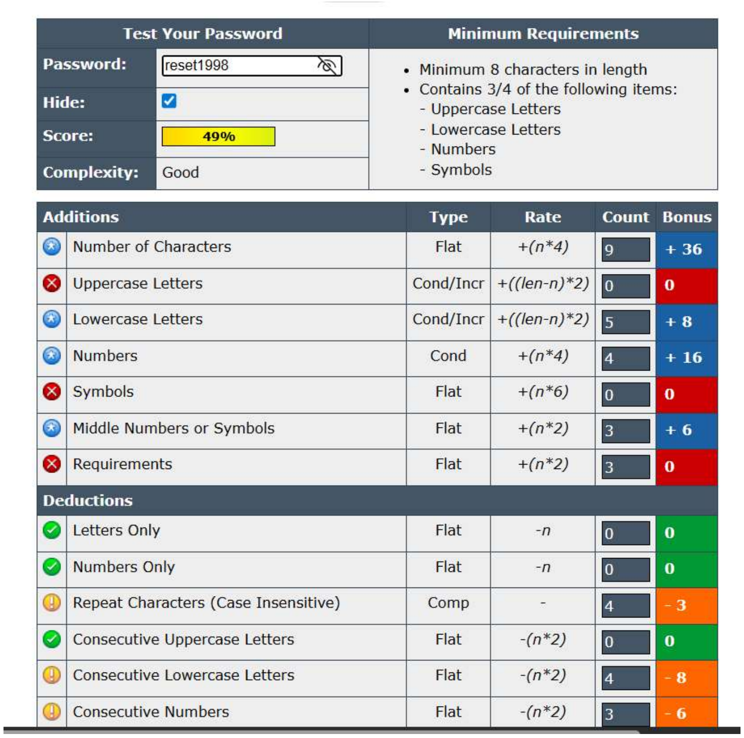
- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
✗	Number of Characters	Flat	+(n*4)	6	+ 24
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	0
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	1	0
	Deductions				
!	Letters Only	Flat	-n	6	- 6
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0

- **Analysis**: This password, "global", received a score of only 7% and was rated as "Very Weak." It is only 6 characters long and consists of only lowercase letters. It received a number of deductions, including for being letters-only and for having consecutive lowercase letters. This password is extremely susceptible to dictionary attacks due to its simplicity and common word usage.

Password 2: "reset1998"

- **Score**: 49%
- **Complexity**: Good
- **Analysis**: This password, "reset1998", received a score of 49% and was rated as "Good." While it meets the minimum requirement of 8 characters in length, it lacks uppercase letters and symbols, which significantly reduces its complexity and strength. It also received deductions for having consecutive lowercase letters and consecutive numbers. This type of password could be susceptible to a dictionary attack, which is a common password attack.



Test Your Password	
Password:	reset1998
Hide:	☑
Score:	49%
Complexity:	Good

Minimum Requirements

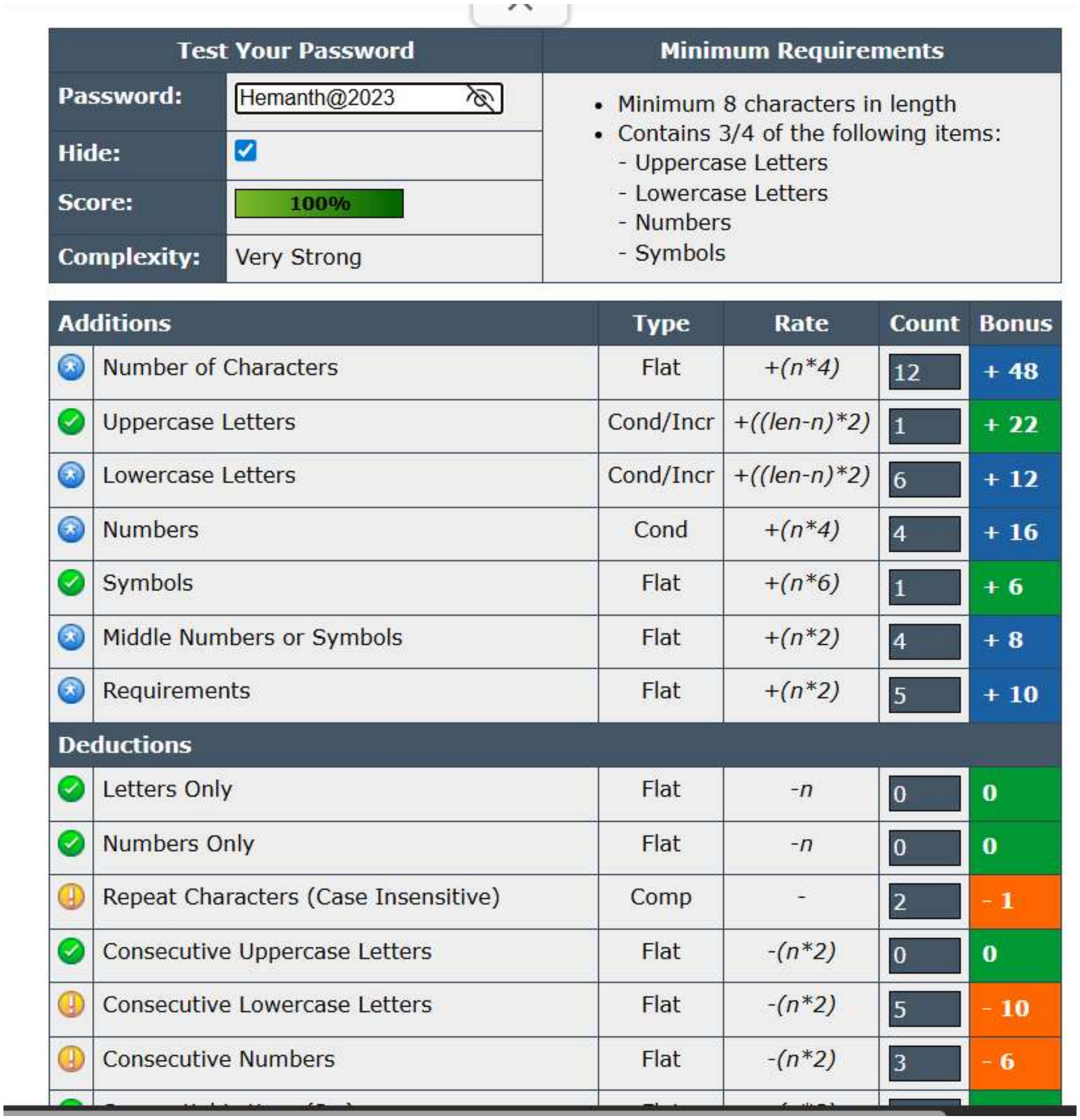
- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	9	+ 36
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 8
★	Numbers	Cond	+(n*4)	4	+ 16
✗	Symbols	Flat	+(n*6)	0	0
★	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
✗	Requirements	Flat	+(n*2)	3	0
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	4	- 3
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
!	Consecutive Numbers	Flat	-(n*2)	3	- 6

Password 3: "Hemanth@2023"

- **Score**: 100%

- **Complexity**: Very Strong
- **Analysis**: This password, "Hemanth@2023", received a perfect score of 100% and was rated as "Very Strong." It meets all the minimum requirements by including a mix of uppercase letters, lowercase letters, numbers, and a symbol. It is 12 characters long, which adds to its complexity. This combination of different character types and its length makes the password much more difficult for common attacks like a brute-force attack.



Test Your Password	
Password:	Hemanth@2023
Hide:	☑
Score:	100%
Complexity:	Very Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	12	+ 48
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 22
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 12
★	Numbers	Cond	+(n*4)	4	+ 16
✓	Symbols	Flat	+(n*6)	1	+ 6
★	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
★	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
!	Consecutive Numbers	Flat	-(n*2)	3	- 6

-

Key Takeaways & Best Practices

Based on this evaluation and additional research, the following key concepts and best practices were identified for creating strong passwords , which are essential for cybersecurity.

- **Password Length**: The length of a password is a critical factor in its strength. Longer passwords are exponentially more difficult for a brute-force attack to crack.
- **Character Diversity**: A strong password must include a variety of character types: uppercase letters, lowercase letters, numbers, and symbols. The use of a mix of characters dramatically increases the number of possible combinations, making it harder for attackers to guess or crack.
- **Avoid Common Patterns**: The passwords "global" and "reset1998" included consecutive numbers and letters, which are common patterns that password cracking tools are designed to detect. Strong passwords should avoid predictable sequences, repeating characters, or easily guessable information.
- **Understanding Common Attacks**: Researching common password attacks, such as brute-force and dictionary attacks, helps in understanding why password complexity is so important for security.
- **Passphrases**: A passphrase is a sequence of random words that can be a great way to create a strong yet memorable password. They are often very long and contain spaces, making them difficult to crack.
- **Password Managers**: Password managers can help by securely generating and storing unique, complex passwords for all your accounts.
- **Multi-Factor Authentication (MFA)**: MFA adds an extra layer of security by requiring a second form of verification in addition to your password. Even if an attacker learns your password, they cannot access your account without the second factor.